

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF GEORGIA  
ATLANTA DIVISION

NATALIE WILLINGHAM, individually,  
and on behalf of all others similarly  
situated,

*Plaintiff,*  
v.

GLOBAL PAYMENTS, INC.,

*Defendant.*

CASE NO.:

CLASS ACTION

JURY TRIAL DEMANDED

**CLASS ACTION COMPLAINT**

Plaintiff, Natalie Willingham, individually and on behalf of all entities and persons similarly situated (the “Class” or “Class Members”), by and through her attorneys, brings this class action Complaint against Defendant, Global Payments, Inc., and alleges:

**NATURE OF THE ACTION**

1. Pursuant to Federal Rules of Civil Procedure 23(a), (b)(2), and (b)(3), Plaintiff brings this consumer class action lawsuit against the Defendant, Global Payments, Inc., for its failure to adequately safeguard and secure its computer systems so as to protect the financial and other personally identifiable information (collectively hereinafter “Personally Identifiable Information” or “PII”) of Plaintiff and Class Members. Plaintiff also brings suit for Defendant’s failure to provide timely notification of and specific information regarding the access by unauthorized third parties to her and class members’ Personally Identifiable Information held by Defendant (hereinafter the “Global Payments’ Data Breach” or “Data Breach”).

2. Global Payments Inc. is a provider of electronic transaction processing services for merchants, Independent Sales Organizations (ISOs), financial institutions, government agencies and multi-national corporations located throughout the United States, Canada, Europe, and the Asia-Pacific region. Global Payments is a Fortune 1000 company and provides processing solutions for credit and debit cards, business-to-business purchasing cards, gift cards, electronic check conversion and check guarantee, verification and recovery including electronic check services, as well as terminal management. As a part of its on-going business operations, Global Payments obtains PII regarding millions of consumers and maintains that PII on its computer storage systems.

3. The present case stems from unauthorized third party access to Global Payments' processing system and computer storage systems. In or before early March 2012, on an exact date known by Defendant, Defendant learned that unauthorized third parties had accessed and obtained PII of Plaintiff and Class Members residing on Defendant's computer storage systems.

4. Despite its duty to expeditiously notify individuals that their PII may have been compromised, Defendant kept its knowledge of the data breach secret from the public until releasing a statement on March 30, 2012, after various websites and news organizations reported the unauthorized access to the public earlier that day. According to this statement, Defendant did not notify consumers regarding this unauthorized access upon learning of it, but instead "engaged external experts in information technology forensics and contacted federal law enforcement." This statement further indicated that Global Payments "promptly notified appropriate industry parties to allow them to minimize potential cardholder impact." Nothing in Global Payments' March 30, 2012, public statement indicates, however, that the company notified consumers of the unauthorized access. Indeed, to date, Plaintiff and the Class Members

have received no specific information from Global Payments regarding circumstances surrounding the unauthorized access.

5. On April 2, 2012, Global Payments created a website entitled [www.2012infosecurityupdate.com](http://www.2012infosecurityupdate.com) ostensibly to provide information to consumers, but the information available on this website as of the filing of this Complaint provides no further details regarding the breach and simply repeats the information provided by the company in previous public statements.

6. Despite the lack of information from Global Payments directly, news reports have indicated that up to 10 million credit card accounts may have been improperly accessed by unauthorized third parties. In a conference call to investors on April 2, 2012, Global Payments CEO Paul Garcia stated that the company had a high degree of confidence that the breach was confined to no more than 1.5 million cardholder accounts and was limited to North America.

7. At least two major credit card issuers, Visa and MasterCard, have also released statements indicating that credit card account information in the possession of Global Payments has been exposed to unauthorized third parties. Furthermore, on April 1, 2012, Visa removed Global Payments from a list of hundreds of companies that it considers to be “compliant service providers,” and according to a report by the Wall Street Journal, “Visa confirmed that it removed the company from the list ‘based on Global Payments’ reported unauthorized access.” This Wall Street Journal report further indicates that “Visa said it has asked Global Payments to submit new validation showing that it complies with industry security standards.”

8. More concerning, according to the source originally reporting the incident, a website entitled Krebs on Security, the unauthorized access allowed third parties to obtain full “Track 1 and Track 2” data, which would have included card holder names and account

numbers, potentially allowing these third parties to create cloned versions of actual credit cards.<sup>1</sup>

During the investor conference call held on April 2, 2012, Global Payments CEO Paul Garcia stated that the breach was limited to “Track 2” data, thereby exposing only credit card account numbers and not card holder names or social security numbers.<sup>2</sup>

9. As a result of Global Payments’ failure to adequately protect and secure Plaintiff’s and Class Members PII, unauthorized third parties have gained access to and obtained account numbers and other PII belonging to Plaintiff and Class Members. Upon information and belief, these unauthorized third parties gained access to Plaintiffs’ and Class Members’ PII for the purpose of stealing it and using it for improper purposes.

10. Defendant’s failure to maintain reasonable and adequate procedures to protect and secure Plaintiff’s and Class Members’ PII, and Defendant’s failure to provide Plaintiff and Class Members with timely information regarding the unauthorized access to their PII, has resulted in Plaintiff and Class Members being placed at grave risk of identity theft and other possible fraud and abuse.

11. Plaintiffs and Class Members will suffer irreversible damage if and when their PII is misused. As a proximate result of the unauthorized access, millions of consumers, including Plaintiff and class members, have had their PII compromised, their privacy invaded, have

---

<sup>1</sup> <http://krebsonsecurity.com/2012/03/mastercard-visa-warn-of-processor-breach/>

<sup>2</sup> “Track 1” and “Track 2” data refers to the information contained on the magnetic strip located on the back of credit cards. This magnetic strip can hold three “tracks” of data, but only the first two tracks, Track 1 and Track 2, are uniformly used in the United States. The specific layout of the “tracks” and the information contained within them are governed by an international standard known in the industry as the ISO/IEC 7813 and by specifications promulgated by the International Air Transportation Association and the American Banking Association. Generally, Track 1 contains more information than Track 2. Track 1 typically contains the cardholder’s name, account information including account number and expiration data, and other discretionary data. Track 2, on the other hand, does not contain the cardholders’ name but only account information, including the account number and expiration date, and other discretionary data.

incurred or will incur out-of-pocket costs and have otherwise suffered economic damages in order to monitor their credit card accounts, credit reports, and other financial information in order to protect their PII from misuse.

12. Plaintiff expressly reserves the right to supplement this Complaint as other information relevant to this action becomes available.

#### **PARTIES, JURISDICITON AND VENUE**

13. Plaintiff, Natalie Willingham, is an individual residing in Olathe, Kansas.

14. Defendant, Global Payments, Inc. is a Georgia Corporation, having its principal place of business in Atlanta, Fulton County, Georgia. Global Payments, Inc. conducts substantial business throughout the country but is headquartered in this judicial district and, upon information and belief, a significant portion of the computer systems used by Global Payments is located in this judicial district.

15. Subject matter jurisdiction exists in this Court under 28 U.S.C. § 1331 because this action arises, in part, under federal law. This Court also has supplemental subject matter jurisdiction over the state law allegations raised in this Complaint as provided by 28 U.S.C. § 1337(a).

16. In addition, this Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d) because this is a class action lawsuit in which the amount in controversy exceeds \$5,000,000, exclusive of interests and costs, and Plaintiff and other members of the putative class are citizens of states other than the state of Georgia, the state in which the Defendant is a citizen.

17. Venue is proper in this judicial district under 28 U.S.C. §1391 (b) and (c) because Defendant conducts and transacts substantial business in this judicial district, a substantial portion of the events and conduct giving rise to the violations complained of in this action

occurred in this judicial district, and Defendant conducts business with consumers in this judicial district.

### **FACTUAL ALLEGATIONS**

18. Global Payments is a publically traded corporation that acts as a “merchant acquirer,” also known as a credit card processor, meaning it is one of the companies responsible for handling transactions when a customer swipes a credit card at a register. Merchant acquirers have contracts with retailers to handle the processing of card transactions, including debit cards, credit cards and gift cards. The retailer sends the consumer’s information to the merchant acquirer, such as Global Payments, who then forwards that information to Visa, MasterCard, or another issuer, who clears the transaction with the consumer’s bank.

19. Merchant acquirers are frequently the target of attacks designed to access and steal PII because they handle transactions for every brand and type of credit card and for banks all over the world. Given this, merchant acquirers are on notice of the need to take heightened security precautions to protect consumers’ PII.

20. In 2011, Global Payments was the seventh-largest merchant acquirer in the United States, according to the Nilson Report, a payments-industry newsletter. Global Payments handled \$120.6 billion in Visa and MasterCard card volume in 2011, up 11% from the prior year, according to Nilson.

21. To process transactions for Visa, MasterCard and other major credit card issuers, merchant acquirers, including Global Payments, must agree by contract to meet certain industry established security standards, including what is known as the Payment Card Industry (PCI) Data Security Standard. The PCI Data Security Standard requires, among other things, an

independent audit of a merchant acquirer's security practices and procedures and periodic reports on compliance by that credit card processor.

22. Visa, MasterCard, and other major credit card issuers maintain lists of merchant acquirers that meet the PCI Data Security Standard. Prior to March 30, 2012, Global Payments was listed by Visa, MasterCard and other major credit card issuers as being PCI Data Security Standard compliant.

23. On or about March 30, an internet security website reported that in "separate non-public alerts sent late last week, VISA and MasterCard began warning banks about specific cards that may have been compromised. The card associations stated that the breached credit card processor was compromised between Jan. 21, 2012 and Feb. 25, 2012. The alerts also said that full Track 1 and Track 2 data was taken – meaning that the information could be used to counterfeit new cards."

24. Later on March 30, the Wall Street Journal reported that Global Payments was the processor involved in the data breach leading to the compromise first reported by the internet website.

25. By the end of the day on March 30, Global Payments issued a public statement acknowledging that it had been the target of an attack and had suffered unauthorized third party access into "a portion of its processing system." Global Payments stated that it had first learned of the unauthorized access in "early March of 2012."

26. On March 31, 2012, Visa announced that it had removed Global Payments from its list of PCI Data Security Standard compliant payment processors.

27. On April 2, 2012, Global Payments held an investor conference call during which CEO Paul Garcia spoke about the unauthorized third party access into Global Payment's

computer systems. Mr. Garcia admitted that the breach involved a “handful” of their servers in their North American system, and that the company was aware that up to 1.5 million card accounts’ information may have been “exported.” Mr. Garcia indicated that the information “exported” was believed to be limited to “track 2” data, and so would not include names or social security numbers of consumers. It was also disclosed during the call that the 1.5 million potentially affected accounts had not been deactivated *en masse* and instead Global Payments would look to the individual issuing institutions to monitor those accounts for fraudulent activity. Mr. Garcia indicated that Global Payments recognized that it would have financial liabilities stemming from its allowing unauthorized access to its customers’ PII.

#### **INDIVIDUAL PLAINTIFF’S ALLEGATIONS**

28. Plaintiff, Natalie Willingham has a Visa branded credit card issued by Bank of America.

29. In mid-March 2012, Ms. Willingham traveled to Minnesota for personal reasons. Upon returning home, she discovered fraudulent charges in the approximate amounts of \$600 and \$300 made to her Bank of America Visa card.

30. Based on the timing of the fraudulent activity on her Bank of America Visa Card, Ms. Willingham believes that her PII was compromised by Defendant through its misconduct outlined herein.

31. Ms. Willingham is particularly upset by reports that Global Payments knew about the breach for a significant amount of time prior to making any information about the breach known to the general public and that to date Global Payments has not provided her with notification of or information regarding the breach.

32. As a result of Defendant's failure to maintain reasonable and adequate procedures to protect and secure Plaintiff's PII and Defendant's failure to provide Plaintiff with timely information regarding the unauthorized access to her PII, Plaintiff has suffered damages, including but not limited to the lost monetary value of her PII, expenses for credit monitoring and identity theft insurance, out-of-pocket expenses, anxiety and emotional distress and loss of privacy.

#### **CLASS ACTION ALLEGATIONS**

33. Plaintiff brings this action on her own behalf and on behalf of all others similarly situated as permitted by Federal Rules of Civil Procedure 23(a), (b)(2), and (b)(3). While the exact number of Class Members is unknown at this time, Plaintiff is informed and believes there are at least 1.5 million members in the proposed class. The proposed class consists of:

**All persons throughout the United States and its territories who had their PII compromised as a result of the Global Payments Data Breach.**

Excluded from the Class are Defendants and any entity in which any Defendant has a controlling interest, and their legal representatives, officers, directors, assignees and successors. Also excluded from the class is any judge to whom this action is assigned, together with any relative of such judge within the third degree of relationship, and the spouse of any such persons.

34. The class is so numerous that joinder of all members is impracticable.

35. The common questions of law and fact among all Class Members predominate over any issues affecting individual Class Members and include the following:

- a. Whether Defendant failed to implement and maintain commercially reasonable procedures to ensure the security of consumers' PII;
- b. Whether Defendant failed to adequately secure PII stored in its processing system;

- c. Whether Defendant took reasonable measures to determine the extent of the security breach;
- d. Whether Defendant's delay in notifying its card-issuer customers of the security breach was unreasonable;
- e. Whether Defendant's delay in informing or failure to inform consumers of the security breach was unreasonable;
- f. Whether Defendant acted negligently in failing to implement and maintain commercially reasonable procedures to secure consumers' PII;
- g. Whether Defendant acted negligently by its delay in informing its card-issuer customers of the security breach;
- h. Whether Defendant acted negligently in delaying or failing to inform consumers of the security breach;
- i. Whether Defendant violated Fair Credit Reporting Act by failing to adopt and maintain reasonable procedures to protect the security of consumers' PII;
- j. Whether Defendant's conduct constitutes negligence;
- k. Whether Defendant's conduct violated the Federal Stored Communications Act;
- l. Whether Defendant's conduct violated O.C.G.A. § 10-1-372;
- m. Whether Defendant's conduct violated O.C.G.A. § 10-1-912;
- n. Whether Plaintiff and Class Members are entitled to injunctive and declaratory relief;
- o. Whether Plaintiff and the Class Members have sustained monetary loss and the proper measure of that loss; and

p. Whether Plaintiff and the Class Members have sustained consequential loss, and, if so, to what measure.

36. Plaintiff will fairly and adequately protect the interests of the class.

37. Plaintiff's claims are typical of those of other Class Members as there are no material differences in the facts and law underlying their claims and Plaintiff's prosecution of their claims will advance the claims of all Class Members.

38. Plaintiff has retained competent counsel experienced in the prosecution of this type of class litigation.

39. Class treatment of the claims set forth in this Complaint is superior to other available methods for the fair and efficient adjudication of this controversy. The expense and burden of individual litigation would make it impracticable or impossible for the proposed Class Members to prosecute their claims individually. Absent a class action, a multiplicity of individual lawsuits would be required to address the claims between the Class Members and the Defendant so that inconsistent treatment and adjudication of the claims would likely result.

40. The litigation and trial of Plaintiff's claims is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the readily ascertainable identities of many Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

41. Adequate notice can be given to Class Members directly using information maintained in Defendant's records or through publication.

42. Damages may be calculated from the information maintained in Defendant's records, so that the cost of administering a recovery for the Class Members can be minimized.

The amount of damages can also be known with precision through Defendant's records or as more specifically defined by the laws cited in this Complaint.

43. Unless a class-wide injunction is issued, Defendant may continue to refuse to provide proper notification to Plaintiff and Class Members regarding the scope of the Data Breach and may continue to act unlawfully as set forth in this complaint.

44. Defendant has acted or refused to act on grounds that apply generally to the class, making final injunctive and declaratory relief appropriate to the class as a whole.

45. Defendant's acts and omissions are the direct and proximate cause of damage described more fully in the succeeding paragraphs of this Complaint.

## **COUNT I**

### **Negligence**

46. Plaintiff repeats and fully incorporates the allegations in paragraphs 1 through 45 above as if fully set forth in this Count on her own behalf and on behalf of the Class Members.

47. Upon accepting Plaintiff's and Class Members' PII through its payment processing services, Global Payments had a duty to exercise reasonable care to secure and safeguard that information and to utilize commercially reasonable methods to do so.

48. Through its acts and omissions described herein, including its failure to provide adequate security and its failure to protect Plaintiff's and Class Members' PII from being captured, accessed, disseminated and misused by third-parties, Defendant unlawfully breached its duty to use reasonable care to protect and secure Plaintiff's and Class Members' PII within its possession or control.

49. Further, through its failure to provide timely and clear notification of the security breach to consumers, Defendant thereby prevented consumers from taking meaningful, proactive

steps to secure their financial data and bank accounts. Defendant unlawfully breached its duty to use reasonable care to protect and secure Plaintiff's and Class Member's PII within its possession of control.

50. Upon information and belief, the PII of Plaintiff and Class Members was improperly and inadequately safeguarded in violation of, *inter alia*, federal and industry rules and regulations at the time of the unauthorized access.

51. Defendant knew or should have known that its computer databases and network for processing Plaintiff's and Class Members' PII and related information had security vulnerabilities. Defendant was negligent in continuing such data processing in light of those vulnerabilities and the sensitivity of the data.

52. Defendant's failure to take proper security measures to protect Plaintiff and Class Members' sensitive PII as described herein created conditions conducive to a foreseeable intervening criminal act, namely the unauthorized access by third parties to consumers' PII stored on Defendant's computer systems.

53. By failing to take proper security measures to protect Plaintiff and Class Members' sensitive PII as described herein, Defendant's conduct was grossly negligent and departed from all reasonable standards of care.

54. Defendant failed to adequately protect its databases from third-party attacks, failed to utilize appropriate encryption techniques, and failed to provide Plaintiff and the Class with prompt and sufficient notice that their sensitive PII had been compromised, thereby breaching its duties to Plaintiff and the Class.

55. Indeed, Defendant had a duty to timely disclose the unauthorized access and theft of the PII to Plaintiff and the Class so that Plaintiff and Class Members could take appropriate

measures to avoid unauthorized charges on their accounts, overdraft or “overlimit” penalties on their credit and bank card accounts, cancel or change account numbers, and monitor their financial account information and credit reports for fraudulent charges.

56. Defendant breached its duty to notify consumers of the unauthorized access by waiting several weeks after learning of the breach to notify consumers and then by failing to provide consumers any information regarding the breach until other press and internet sites first began reporting it. To date, Defendant has not provided sufficient information to consumers regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiff and the Class.

57. Neither Plaintiff nor the other members of the Class contributed to the security breach described herein or to the unauthorized access of their sensitive PII.

58. As a direct and proximate cause of Defendant’s conduct, Plaintiff and the Class suffered damages including, but not limited to, monetary loss for fraudulent charges; interest or overdraft or “overlimit” penalties on their accounts; fear and apprehension of fraud, abuse, loss of money, and identity theft; the burden and cost of monitoring their credit, bank accounts and credit history; the burden and cost of closing compromised accounts and opening new accounts; the burden of closely scrutinizing credit card statements for past and future transactions; damages to their credit history; loss of privacy; and other economic damages.

**COUNT II**

**Violation of the Federal Stored Communications Act  
18 U.S.C. § 2702**

59. Plaintiff repeats and fully incorporates the allegations in paragraphs 1 through 45 above as if fully set forth in this Count on her own behalf and on behalf of the Class Members.

60. The Stored Communications Act (“SCA”) provides consumers with redress if a company mishandles their electronically stored information. The SCA was designed, in part, to protect individuals’ privacy interests in personal and proprietary information.

61. Section 2702(a)(1) of the SCA provides “a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service.” 18 U.S.C. § 2702(a)(1).

62. The SCA defines “electronic communication service” as “any service which provides to users thereof the ability to send or receive wire or electronic communications.” 18 U.S.C. § 2510(15).

63. Through its payment processing equipment, Defendant provides an “electronic communication service to the public” within the meaning of the SCA because it provides consumers with payment processing services that enable consumers to send wire or electronic communications concerning their accounts to financial institutions processing credit card and other electronic payments.

64. By failing to take commercially reasonable steps to safeguard Plaintiff and Class Members’ sensitive PII while in electronic storage, Defendant has allowed unauthorized access to its processing system and knowingly divulged customer credit and debit account information.

65. Section 2702(a)(2)(A) of the SCA provides “a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service on behalf of, and received by means of electronic transmission from (or created by means of computer processing or

communications received by means of electronic transmission from), a subscriber or customer of such service.” 18 U.S.C. § 2702(a)(2)(A).

66. The SCA defines “remote computing service” as “the provision to the public of computer storage or processing services by means of an electronic communications system.” 18 U.S.C. § 2711(2).

67. The SCA defines “electronic communications system” as “any wire, radio, electromagnetic, photo-optical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications.” 18 U.S.C. § 2510(14).

68. Defendant provides remote computing services to the public by virtue of its payment processing services for consumer credit and debit card payments, which are used by consumers and carried out by means of an electronic communications system, including online systems that accept user inputs for computer storage and processing services. Defendant stores personal and financial information on behalf of the public and utilizes such information to process its services on behalf of consumers and financial institutions processing credit card and other electronic payments.

69. By failing to take commercially reasonable steps to safeguard sensitive consumer financial data and PII and allowing its computer systems to be breached, Defendant knowingly divulged consumer credit and debit account information, which was carried and maintained on Defendant’s remote computing service, and which allowed unauthorized third parties to duplicate consumers’ credit cards.

70. Upon learning that its servers and computer storage systems had been intruded upon and information had been obtained and accessed by third-parties, Defendant failed to

inform Plaintiff and the Class of the security breach and continued to knowingly divulge PII to third-parties.

71. As a result of Defendant's conduct described herein and its violations of the SCA, Plaintiff and Class members have suffered injuries described herein including, but not limited to, lost money and the costs associated with the need for vigilant credit monitoring to protect against additional identity theft, Plaintiff and the Class seek judgment in their favor against Defendant awarding them the maximum statutory damages available under 18 U.S.C. § 2707, including punitive damages for willful or intentional violations.

### **COUNT III**

#### **Willful Violation of the Fair Credit Reporting Act 15 U.S.C. §1681, et seq.**

72. Plaintiff repeats and fully incorporates the allegations in paragraphs 1 through 45 above as if fully set forth in this Count on her own behalf and on behalf of the Class Members.

73. FCRA defines a "consumer report" as "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or collected in whole or in part for the purpose of establishing the consumer's eligibility for (A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes, or (C) any other purpose authorized under section 1681b of this title.

74. Defendant is a "consumer reporting agency" as defined by FCRA in that, on a cooperative nonprofit basis and/or for monetary fees, Defendant regularly engages in the practice of assembling information on consumers for the purpose of furnishing consumer reports to third

parties, and uses interstate commerce for the purpose of preparing or furnishing consumer reports. 15 U.S.C. § 1681a(f).

75. The Fair Credit Reporting Act (FCRA) requires consumer reporting agencies to adopt and maintain reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance and other information in a manner fair and equitable to consumers while maintaining the confidentiality, accuracy, relevancy and proper utilization of such information. 15. U.S.C. § 1681(b).

76. In addition, under FCRA, a consumer reporting agency may only furnish a consumer report to another for a permissible purpose enumerated under 15 U.S.C. § 1681b.

77. Defendant violated FCRA by failing to adopt and maintain reasonable procedures pursuant to 15 U.S.C. § 1681(b), including procedures to adequately secure its servers and computer storage systems, in a manner fair and equitable to consumers while maintaining the confidentiality, accuracy, relevancy and proper utilization of such information. In addition, Defendant violated FCRA because, by its failure to maintain reasonable procedures, unauthorized third parties gained unauthorized access to consumer report information absent a permissible purpose.

78. Defendant's failure to adopt and maintain reasonable procedures in compliance with FCRA was willful.

79. As a result of Defendant's willful violation of FCRA, Plaintiff's and Class Members' PII was accessed by third parties who gained unauthorized access to the information contained on Defendant's computer systems.

80. Plaintiff and Class Members suffered actual damages as a result of Defendant's willful violation of FCRA including but not limited to the lost monetary value of their personal

customer account information, expenses for credit monitoring and identity theft insurance, out-of-pocket expenses, anxiety and emotional distress and loss of privacy.

81. Plaintiff and Class Members are entitled to compensation for their actual damages as described above, or statutory damages of not less than \$100 and not more than \$1000 for Plaintiff and each Class Member, punitive damages in an amount to be established by the Court and attorneys' fees and costs, pursuant to 15 U.S.C. § 1681n(a).

**COUNT IV**

**Negligent Violation of the Fair Credit Reporting Act  
15 U.S.C. §1681 et seq.**

82. Plaintiff repeats and fully incorporates the allegations in paragraphs 1 through 45 above as if fully set forth in this Count on her own behalf and on behalf of the Class Members.

83. Defendant owed a duty to Plaintiff and Class Members to safeguard the security of their personal customer account information and to adopt and maintain reasonable procedures pursuant to 15 U.S.C. § 1681(b), including procedures to adequately secure its servers and sufficiently encrypt its passwords, in a manner fair and equitable to consumers while maintaining the confidentiality, accuracy, relevancy and proper utilization of such information.

84. Defendant negligently failed to adopt and maintain reasonable procedures in a manner fair and equitable to consumers while maintaining the confidentiality, accuracy, relevancy and proper utilization of such information in compliance with FCRA. In addition, Defendant negligently violated FCRA because, by its failure to maintain reasonable procedures, hackers gained unauthorized access to consumer report information absent a permissible purpose.

85. Plaintiff and Class Members suffered actual damages as a result of Defendant's willful violation of FCRA including but not limited to the lost monetary value of their personal

customer account information, expenses for credit monitoring and identity theft insurance, out-of-pocket expenses, anxiety and emotional distress and loss of privacy.

86. Plaintiff and Class Members are entitled to compensation for their actual damages as described above, and attorneys' fees and costs, pursuant to 15 U.S.C. § 1681o(a).

## **COUNT V**

### **Violations of Georgia's Unfair and Deceptive Trade Practices Act O.C.G.A. § 10-1-372**

87. Plaintiff repeats and fully incorporates the allegations in paragraphs 1 through 45 above as if fully set forth in this Count on her own behalf and on behalf of the Class Members.

88. O.C.G.A. § 10-1-372 (hereinafter "UDTPA") is expressly intended to protect "persons" from potentially confusing or deceptive trade practices.

89. Defendant is a "person" within the meaning of the UDTPA and, at all pertinent times, was subject to the requirements and proscriptions of the UDTPA with respect to all of their business and trade practices described herein.

90. Plaintiff and Class Members are "persons" "likely to damaged" by Defendant's ongoing deceptive trade practices.

91. Defendant's unlawful conduct as described herein arose, was directed, and emanated from Defendant's headquarters in Atlanta, Georgia to the detriment of Plaintiff and Class Members in Georgia and throughout the United States.

92. Defendant violated the UDTPA by failing to properly implement adequate, commercially reasonable security measures to protect consumers sensitive PII.

93. Defendant also violated the UDTPA by failing to immediately notify affected customers of the nature and extent of the security breach, as required by O.C.G.A. § 10-1-912 and various other state data breach notification statutes.

94. Defendant represents its services as a particular standard and quality, which allows it to provide a safe and secure environment for the transmission of consumers' financial information. Contrary to this representation, Defendant failed to properly implement adequate, commercially reasonable security measures to protect consumers' sensitive PII, and to protect the loss and misuse of this information.

95. Defendant also represents that its services have the characteristics, ingredients, uses and benefits of providing a safe and secure environment for the transmission of consumers' financial information. Contrary to this representation, Defendant failed to establish adequate safeguards to protect consumers' sensitive PII, failed to maintain this sensitive PII in an adequately encrypted database and failed to maintain reasonable security measures to protect the loss and misuse of this PII.

96. Plaintiff and Class Members have suffered ascertainable losses as a direct result of Defendant's employment of unconscionable acts or practices, and unfair or deceptive acts or practices.

97. Pursuant to the Georgia's UDTPA, Plaintiff and the Class are entitled to preliminary and permanent injunctive relief without proof of monetary damage, loss of profits, or intent to deceive. Plaintiff and the Class seek equitable relief and to enjoin Defendants on the terms that the Court considers reasonable.

98. Defendant's conduct caused and continues to cause substantial injury to Plaintiff and Class members. Unless preliminary and permanent injunctive relief is granted, Plaintiff and the Class will suffer irreparable harm. Plaintiff and the Class do not have an adequate remedy at law. The balance of the equities weighs in favor of Plaintiff and the Class.

99. At all material times, Defendant's deceptive trade practices were willful within the meaning of the UDTPA and, accordingly, Plaintiff and the Class are entitled to an award of attorneys' fees, costs and other recoverable expenses of litigation.

**COUNT VI**

**Negligence Per Se**

100. Plaintiff repeats and fully incorporates the allegations in paragraphs 46 through 58 and 60 through 71, 73 through 81, 83 through 86 and 88 through 99 above as if fully set forth in this Count on her own behalf and on behalf of the Class Members.

101. Defendant's violations of the Stored Communications Act, 18 U.S.C. § 2702, Fair Credit Reporting Act 15 U.S.C. §1681, et seq., O.C.G.A. § 10-1-372 and O.C.G.A. § 10-1-912 resulted in injury to Plaintiff and the Class.

102. The harm Defendant caused to Plaintiff and the Class are injuries that result from the type of occurrences those statutes were designed to prevent.

103. Plaintiff and the Class are the type of persons for whose protection those statutes were adopted.

104. Defendant's violations of the foregoing statutes as described herein resulted in injury to Plaintiff and the Class.

**COUNT VII**

**Breach of Third Party Beneficiary Contract**

105. Plaintiff repeats and fully incorporates the allegations in paragraphs 1 through 45 above as if fully set forth in this Count on her own behalf and on behalf of the Class Members.

106. Defendant came into possession of Plaintiff's and Class Members' PII for the sole purpose of processing purchases and contracted to protect such information.

107. Upon information and belief, the contract between merchants, banks and other card issuing entities and Defendant (“Processing Contract”) requires Defendant to not disclose Plaintiff’s and Class Members’ PII to unauthorized third party entities and to safeguard and protect PII from being stolen.

108. Upon information and belief, this Processing Contract requires, among other things, for Defendant to employ commercially reasonable efforts to preserve the security and confidentiality of consumer’s PII under its control and to prevent the unauthorized or unlawful access to this PII.

109. Because Defendant failed to safeguard and protect the PII of Plaintiff and the Class from being compromised or stolen, Defendant breached its Processing Contract with merchants, banks and other card issuing entities pursuant to which Plaintiff and Class Members were third party beneficiaries.

110. Upon information and belief, Defendant breached the Processing Contract by not meeting the minimum level of protecting consumers’ PII and by failing to prevent the unauthorized access and theft of Plaintiff’s and Class Members’ PII.

111. As a direct and proximate result of Defendant’s conduct, Plaintiff and the Class suffered damages including, but not limited to, monetary loss for fraudulent charges, interest or overdraft or “overlimit” penalties on their accounts; fear and apprehension of fraud, abuse, loss of money, and identity theft; the burden and cost of monitoring their credit, bank accounts and credit history; the burden and cost of closing compromised accounts and opening new accounts; the burden of closely scrutinizing credit card statements for past and future transactions; damage to their credit history; loss of privacy; and other economic damages.

**COUNT VIII**

**Breach of Implied Contract**

112. Plaintiff repeats and fully incorporates the allegations in paragraphs 1 through 45 above as if fully set forth in this Count on her own behalf and on behalf of the Class Members.

113. Global Payments provides electronic payment processing services, including total processing capabilities (and end-to-end payment solutions) for credit, debit, Electronic Benefits Transfer (EBT), gift, loyalty and purchasing cards for all major card types and technologies. In practice, this means that when a consumer swipes one of these cards at a card reader, the sensitive PII is encrypted and can be stored and transmitted to a processor, such as Defendant, who then forwards that information to Visa, MasterCard, or another issuer, who clears the transaction with the consumer's bank.

114. By providing such sensitive PII to Defendant, and upon Defendant's acceptance of such information, Plaintiff and the Class, on the one hand, and Defendant, on the other hand, entered into implied contracts whereby Defendant was obligated to reasonably secure and safeguard that information.

115. Without such implied contracts, Plaintiff and the Class would not have provided their personal information to Defendant.

116. Defendant breached the implied contract with Plaintiff and members of the Class by failing to properly secure Plaintiff and the Class's sensitive PII and by failing to take reasonable measures to safeguard the sensitive PII.

117. Defendant was further obligated to provide Plaintiff and the Class prompt, adequate notice of any security breach or unauthorized access of said information.

118. Defendant breached its implied contract with Plaintiff and Class members by failing to provide prompt, adequate notice of the security breach and unauthorized access of customer financial information.

119. Defendant's breach and other misconduct described herein resulted in injury to Plaintiff and the Class. Plaintiff and the Class members did not receive the benefit of the bargain for which they contracted and for which they paid valuable consideration in the form of their personal information.

120. Plaintiff and Class members suffered and will continue to suffer damages including, but not limited to loss of their financial information, loss of money and costs incurred as a result of increased risk of identity theft, and other economic and noneconomic harm, all of which have ascertainable value to be proven at trial.

**RELIEF SOUGHT**

**FOR ALL THESE REASONS**, Plaintiff, Natalie Willingham, individually and on behalf of all others similarly situated, seeks relief as more fully set forth in this Complaint as follows:

- a. For an order certifying that the action may be maintained as a class action, under Rule 23, Federal Rules of Civil Procedure and certifying Plaintiff, Natalie Willingham, as Class Representative, and designating her counsel as counsel for the class;
- b. Finding that Defendant breached its duty to safeguard and protect Plaintiff's and Class Members' PII processed or stored on Defendant's computer network;
- c. For an award of equitable relief as follows:

- i. Enjoining Defendant from engaging in similar unfair, unlawful, deceptive, and fraudulent misconduct in the future;
- ii. Requiring Defendant to make full restitution of all monies wrongfully obtained as a result of the wrongful conduct described in this Complaint;
- iii. Requiring Defendant to disgorge all ill-gotten gains flowing from the wrongful conduct described in this Complaint;
- iv. Requiring Defendant to engage in a correct notice campaign;
- d. For an award of attorney's fees and costs;
- e. For an award of statutory damages under the applicable statutes to be determined at trial;
- f. For an award of damages to be determined at trial; and
- g. For any further legal and equitable relief as this Court may deem just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiff demands a trial by jury on issues so triable.

Dated April 4, 2012

Respectfully submitted,

/s/ Justin D. Miller  
**JUSTIN D. MILLER, ESQUIRE**  
Georgia Bar No. 001307  
MORGAN & MORGAN, P.A.  
191 Peachtree St. NE  
Suite 4200

Atlanta, GA 30303-1748  
Telephone: (404) 965-8823  
Facsimile: (404) 965-8812  
Email: [jdmiller@forthepeople.com](mailto:jdmiller@forthepeople.com)

**J. ANDREW MEYER, ESQUIRE**  
Florida Bar No. 0056766  
**TAMRA GIVENS, ESQUIRE**  
Florida Bar No. 657638  
**RACHEL SOFFIN, ESQUIRE**  
Florida Bar No. 0018054  
Georgia Bar No. 255074  
**MORGAN & MORGAN, P.A.**  
201 North Franklin Street  
7<sup>th</sup> Floor  
Tampa, Florida 33602  
Telephone: (813) 223-5505  
Facsimile: (813) 223-5402  
Email: [ameyer@forthepeople.com](mailto:ameyer@forthepeople.com)  
[tgivens@forthepeople.com](mailto:tgivens@forthepeople.com)  
[rsoffin@forthepeople.com](mailto:rsoffin@forthepeople.com)

**SCOTT WM WEINSTEIN, ESQUIRE**  
Florida Bar No. 563080  
**MORGAN & MORGAN, P.A.**  
12800 University Drive, Suite 600  
Fort Myers, FL 33907-5337  
Telephone: (239) 433-6880  
Facsimile: (239) 433-6836  
Email: [sweinstein@forthepeople.com](mailto:sweinstein@forthepeople.com)